

UNITED STATES DISTRICT COURT

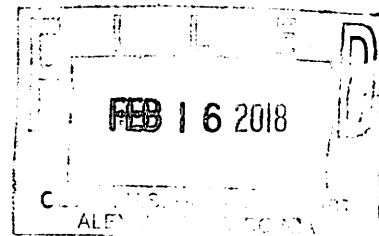
for the
Eastern District of Virginia

UNDER SEAL

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 1:18-sw-94

INFORMATION ASSOCIATED WITH:
lisahshapiro@aol.com THAT IS STORED AT
PREMISES CONTROLLED BY AOL



APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

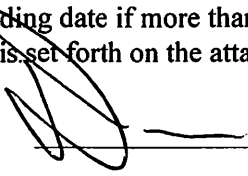
The search is related to a violation of:

Code Section
18 U.S.C. § 1030

Offense Description
Unauthorized computer access and computer-related fraud

The application is based on these facts:
See attached affidavit


- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Donald L. Cavender, Special Agent - FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: FEB. 16, 2018

 /s/ 
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

The Honorable John F. Anderson, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with **lisahshapiro@aol.com** from inception to present that is stored at premises controlled by AOL, a company that accepts service of legal process at **AOL Inc./Oath Inc. Legal Process, 22000 AOL Way, Dulles, VA 20166.**

ATTACHMENT B

**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

I. Information to be disclosed by AOL (the “Provider”) to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on 12/11/2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, dating from the initiation of the account to the present, including stored or preserved copies of e-mails sent to and from the account, e-mail attachments, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including content of all AOL services to include AOL services and any other AOL services enabled and associated with the AOL accounts subscribers above.

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to: dlcavender@fbi.gov

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 1030 (Unauthorized Computer Access and Computer-Related Fraud), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The content of any and all electronic communication, and any internet search history, other internet activity, or documents, that pertains to:
- (b) Evidence of unauthorized collection of email accounts, or the impersonation of other individuals via email, or the registration of domain names to further fraudulent activity;
- (c) Computer Intrusion Activity in all of its forms, including but not limited to the purchase of or development/execution of malware, control/sale of command and control servers, and control of computer credentials;
- (d) Motive for computer intrusion activity;
- (e) The illegal trafficking of personal identifying information, usernames and passwords of compromised computers or internet accounts, or any other items which are being offered, requested, or possessed without the authorization of the bona fide owner;
- (f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the email account owner's state of mind as it relates to the criminal activity under investigation;

- (h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (i) The identity of the person(s) who communicated with the user IDs about matters relating to unauthorized collection of email accounts, or the impersonation of other individuals via email, or the registration of domain names to further fraudulent activity, including records that help reveal their whereabouts.
- (j) The identity of the user of the account(s), to include (but not limited to) names, location of the user, passwords, IP addresses, email communications with other internet accounts (whether email, domain, or any other) under the control of the user.
- (k) Any and all records or other information pertaining to the identity of the subscriber of the Target Account, including but not limited to associated email accounts, login IP addresses, and session times and durations.
- (l) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (m) Evidence indicating the email account owner's state of mind as it relates to the criminal activity under investigation;
- (n) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (o) Identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses;

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

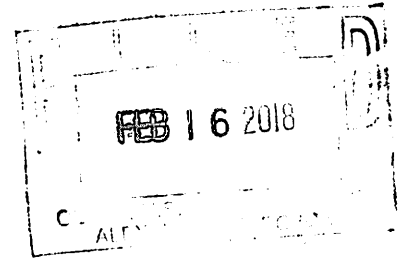
Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

UNDER SEAL

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH:
lisahshapiro@aol.com
THAT IS STORED AT PREMISES
CONTROLLED BY AOL

1:18-sw-94
Filed Under Seal



**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Donald L. Cavender, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by AOL, an e-mail provider headquartered at **AOL Inc./Oath Inc. Legal Process, 22000 AOL Way, Dulles, VA 20166**. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require AOL to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since March, 1990. During that time, I have received training and gained experience in computer crime investigations and digital forensics. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search and seizure warrants,

and the identification and collection of computer-related evidence. I am currently assigned to the criminal cyber-crime squad of the FBI Washington Field Office. I was assigned for over three years as a computer crime instructor at the FBI Academy at Quantico, VA and taught FBI Agents and Task Force Officers in cyber-crime investigation and E-mail tracing. I conducted research on topics relevant to cyber-crime and provided case consultation to FBI Field Offices.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030 (Unauthorized Computer Access and Computer-Related Fraud), (hereinafter the “Targeted Offenses”) have been committed by as yet unknown persons in control of the above email account. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within the Eastern District of Virginia. *See* 18 U.S.C. § 3237. *See* 18 U.S.C. § 3238.

PROBABLE CAUSE

6. On December 8, 2017, the affiant with Special Agent Amanda Fritz interviewed MIKE RUNNHEIM, Enterprise Infrastructure Architect for K2M, was interviewed at his place of employment, K2M, 600 Hope Parkway SE, Leesburg, VA. Also present for the interview were LEE LOWDER, Vice President-Compliance for K2M, JEFF GURGAMUS, Vice President of Finance and Treasury for K2M, and PETE SCHaubACH, Chief Information Officer for K2M (via conference call). RUNNHEIM provided the following information:

7. K2M's servers are hosted at Equinox Data Center. K2M uses Office 365 for its email service. The company migrated to Office 365 in 2013 and purchased the E3 licensing, which was the middle tier of licenses. With the E3 licensing, K2M was able to retrieve the source IP logs for the past 30 days. They have preserved these logs.

Dr. KOSTUIK's Email Account

8. The Founder and Chief Scientific Officer for K2M is Dr. JOHN KOSTUIK. Dr. KOSTUIK is believed to be in his 80s but remains active within the company. On 11/28/17, Dr. KOSTUIK was having trouble with sending emails (he received several "delivery error notifications") and contacted the K2M IT department to look at it. RUNNHEIM noted that a large amount of emails were being sent from Dr. KOSTUIK's email account. RUNNHEIM discovered that there was a rule set in Dr. KOSTUIK's email account to forward all emails received to email address "isewquiltss@gmail.com". The rule did not include any filters or key words, therefore, all of the emails received in Dr. KOSTUIK's email inbox was being forwarded to isewquiltss@gmail.com. RUNNHEIM contacted Dr. KOSTUIK's assistant, and asked if Dr. KOSTUIK used the email address isewquiltss@gmail.com to which she confirmed that the email

address was not his and he had never used it. On 12/05/2017, RUNNHEIM turned off and deleted the rule in Dr. KOSTUIK's email account.

9. I know from training and experience that cyber criminals will create email accounts for the sole purpose of receiving forwarded emails from compromised systems, where inbox rules were created to forward email from the compromised systems to their email accounts. Cyber criminals monitor the forwarded emails for opportunities to conduct fraudulent activities.

10. RUNNHEIM ran a script to check all K2M email accounts for forwarding rules to outside email addresses and did not find any other accounts with a suspicious rule established. Some email accounts had rules created but most rules were to move emails to certain folders, etc. None of the rules created forwarded emails to an outside email account.

11. RUNNHEIM conducted a mail trace, which was able to pull data for the past 90 days, for Dr. KOSTUIK's email account and he noted that the first forwarded email to isewquiltss@gmail.com occurred on 09/29/2017. As such, the rule was added to either Dr. KOSTUIK's Outlook program on his computer or from Outlook Web Access sometime before the email was forwarded. RUNNHEIM verified with Microsoft that the date that a rule was created was not logged.

12. Dr. KOSTUIK utilizes his iPhone, iPad, and laptop computer to access his K2M email account. Dr. KOSTUIK had not changed the password to access his K2M account in a very long time. Furthermore, his iPad was not password protected; however, Dr. KOSTUIK had all of these items in his possession around the time the rule was believed to have been created. Since the discovery of the rule in his account, Dr. KOSTUIK changed all of his passwords and all of his devices are now password protected. RUNNHEIM had not yet found the vector for

accessing Dr. KOSTUIK's account. RUNNHEIM had not reviewed Dr. KOSTUIK's email account for any suspicious spam emails.

13. K2M was not a victim of any financial loss associated with the unauthorized access into Dr. KOSTUIK's account; however, Dr. KOSTUIK received many emails containing company sensitive and proprietary information, including proposed fiscal year 2018 R&D projects and 2018 financial plan. If this data was released to the public, it could result in the loss of hundreds of millions of dollars to the company if disclosed. Furthermore, Dr. KOSTUIK utilized his K2M email account for personal reasons and his personal financial data could be found in the account. Dr. KOSTUIK's wife contacted their financial institutions and it did not appear that any of them had been used fraudulently.

14. Upon discovery of the forwarding rule on Dr. KOSTUIK's laptop, the K2M IT department performed a basic forensic analysis of the laptop. Nothing was deleted from the laptop as a result of the forensic analysis conducted. The K2M IT department did not find any unusual files or anything suspicious on the laptop. They reviewed the logs and viewed the system settings to see if any executable files were dropped on it, but none were located.

15. K2M had not yet implemented two-factor authentication for logging into its system. K2M uses "Octa" for signing into the system. They indicated that in the following week, management planned to review implementing a new two-factor authentication system.

16. RUNNHEIM showed the Agents the log for Dr. KOSTUIK's successful logins for the period 11/09/17 – 12/04/17. RUNNHEIM pointed out that on 11/13/17 and 11/15/17, Dr. KOSTUIK's account was accessed from the Windows10, Firefox client; however, Dr. KOSTUIK's laptop had not yet been upgraded from Windows 7 to Windows 10. Furthermore, on 11/13/2017, the user's location showed Denton, TX and on 11/15/17, the user's location

showed Florissant, MO but Dr. KOSTUIK was not at those locations on those dates. LARRY DOOLEY, Vice President of National Accounts and Pricing for K2M, resides in Denton, TX and attended a conference in Missouri on 11/15/17. Additionally, DOOLEY uses a Microsoft Surface to access his K2M account and the Surface has Windows 10 installed on it. DOOLEY's account also had suspicious activity the past month or so.

LARRY DOOLEY's Email Account

17. Two suspicious and fraudulent emails have been sent to the Accounts Payable and Payroll departments at K2M pretending to be from LARRY DOOLEY asking for payment of an invoice and to change his bank information for his paychecks. The first email impersonating DOOLEY was sent to the Accounts Payable department. In the spoofed email, "DOOLEY" requested that payment be issued for a particular invoice. The AP employee, KAREN (not further identified), replied back to the email stating that the payment would first have to be approved by the appropriate managers. The invoice was not paid.

18. On 11/14/2017, a second spoofed email impersonating DOOLEY was sent to the Payroll department. In the email, "DOOLEY" stated that he was having trouble with his bank and wanted to have his paychecks deposited to another bank account. The new bank account information was included in the email. Upon discovery of the spoofed email, the company contacted the new bank and notified the bank of the fraud and to freeze the account. RUNNHEIM reviewed the email received by the Payroll department from "DOOLEY" and noticed that the email was sent from email address lisahshapiro@aol.com (the "TARGET AOL ACCOUNT").

19. As a result of the spoofed emails, DOOLEY has changed all of his passwords. The proxy on DOOLEY's computer is ZScaler. K2M currently uses Cylance for virus

protection. The company also previously used E-Sec for virus protection; however, E-Sec was removed in November 2017 because it was discovered that Cylance and E-Sec competed and worked against each other.

20. LOWDER identified K2M as the owner of the laptop computer used by Dr. KOSTUIK. Dr. KOSTUIK's laptop computer is a Dell Latitude E7240, Serial # DPNNFG6JA00. Under a written and signed consent to search authorization, LOWDER and RUNNHEIM provided the laptop computer to the FBI for forensic examination.

21. K2M also gave consent to the FBI to image and search DOOLEY's Surface; however, K2M was not in possession of DOOLEY's Surface but would obtain it from him. On 12/13/2017, LOWDER contacted SA Fritz to notify her that DOOLEY's Surface was ready to be released to the FBI. On 12/13/2017, LOWDER provided DOOLEY's Microsoft Surface, Serial #013003743653, to SA Fritz and LOWDER once again provided written and signed consent on behalf of K2M.

22. On 12/08/2017, RUNNHEIM emailed to SA Fritz the login logs and message trace reports for Dr. KOSTUIK's and DOOLEY's email accounts as well as a screenshot of the rule created in Dr. KOSTUIK's email account to forward all emails to the email address isewquiltss@gmail.com.

23. On December 11, 2017, the affiant requested the preservation of the TARGET AOL ACCOUNT to AOL. In general, an e-mail that is sent to a AOL subscriber is stored in the subscriber's "mail box" on AOL servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on AOL servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on AOL's servers for a certain period of time.

BACKGROUND CONCERNING E-MAIL

24. In my training and experience, I have learned that AOL provides a variety of on-line services, including electronic mail (“e-mail”) access, to the public. AOL allows subscribers to obtain e-mail accounts at the domain name aol.com, like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with AOL. During the registration process, AOL asks subscribers to provide basic personal information. Therefore, the computers of AOL are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for AOL subscribers) and information concerning subscribers and their use of AOL services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

25. An AOL subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by AOL. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

26. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such

information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often nevertheless provides clues to their identity, location, or illicit activities.

27. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

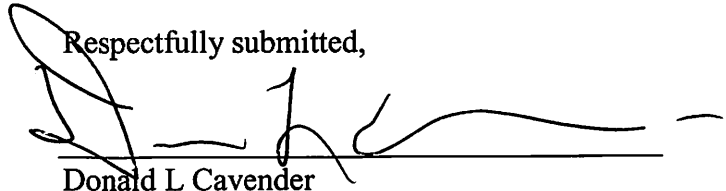
28. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each offense-element, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Finally, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on **AOL** who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Donald L Cavender
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on Feb. 16, 2018

/s/ JFO
HONORABLE JOHN F. ANDERSON
United States Magistrate Judge
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with **lisahshapiro@aol.com** from inception to present that is stored at premises controlled by AOL, a company that accepts service of legal process at **AOL Inc./Oath Inc. Legal Process, 22000 AOL Way, Dulles, VA 20166.**

ATTACHMENT B

**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

I. Information to be disclosed by AOL (the “Provider”) to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on 12/11/2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, dating from the initiation of the account to the present, including stored or preserved copies of e-mails sent to and from the account, e-mail attachments, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including content of all AOL services to include AOL services and any other AOL services enabled and associated with the AOL accounts subscribers above.

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to: dlcavender@fbi.gov

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 1030 (Unauthorized Computer Access and Computer-Related Fraud), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The content of any and all electronic communication, and any internet search history, other internet activity, or documents, that pertains to:
- (b) Evidence of unauthorized collection of email accounts, or the impersonation of other individuals via email, or the registration of domain names to further fraudulent activity;
- (c) Computer Intrusion Activity in all of its forms, including but not limited to the purchase of or development/execution of malware, control/sale of command and control servers, and control of computer credentials;
- (d) Motive for computer intrusion activity;
- (e) The illegal trafficking of personal identifying information, usernames and passwords of compromised computers or internet accounts, or any other items which are being offered, requested, or possessed without the authorization of the bona fide owner;
- (f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the email account owner's state of mind as it relates to the criminal activity under investigation;

- (h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (i) The identity of the person(s) who communicated with the user IDs about matters relating to unauthorized collection of email accounts, or the impersonation of other individuals via email, or the registration of domain names to further fraudulent activity, including records that help reveal their whereabouts.
- (j) The identity of the user of the account(s), to include (but not limited to) names, location of the user, passwords, IP addresses, email communications with other internet accounts (whether email, domain, or any other) under the control of the user.
- (k) Any and all records or other information pertaining to the identity of the subscriber of the Target Account, including but not limited to associated email accounts, login IP addresses, and session times and durations.
- (l) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (m) Evidence indicating the email account owner's state of mind as it relates to the criminal activity under investigation;
- (n) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (o) Identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses;

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by AOL, and my official title is _____. I am a custodian of records for AOL. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of AOL, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of AOL; and
- c. such records were made by AOL as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature